Gowers一様性による剰余関数と多項式の相関の評価 (理論計算機科学の深化 : 新たな計算世界観を求めて)

AUTHOR(S):

田中, 秀宗; 河内, 亮周

数理解析研究所講究録
第1599巻 2008年 133-140

Gowers一様性による剰余関数と多項式の相関の評価

田中 秀宗 (Hidetoki Tanaka)　　河内 亮周 (Akinori Kawachi)
東京工業大学 数理・計算科学専攻
Department of Mathematical and Computing Sciences, Tokyo Institute of Technology
Email:{tanaka7,kawachi}@is.titech.ac.jp

概要

関数 f と関数のクラス C との相関は，f の C に対する平均的な難しさを表す尺度である．特に，剰余関数と低次多項式のクラスとの相関は，回路計算量とも関係が深く，重要な概念である．Viola と Widgerson によって，GF(2) 上の Gowers 一様性がこの相関の評価に導入され，指数関数的な上界が示された．本研究では，相関評価に GF(3) 上の Gowers 一様性を導入し，MOD_m 関数と GF(3) 上の d 次多項式の相関の上界が $\exp(-\Omega(n/3^d))$ であることを示した．この結果は，従来示されていたの上界の特殊ケースにおける改善となっている．また，この結果はある形の閾値回路の下界を含意している．

1 序論

関数 $f:\{0,1\}^n \to \{1,-1\}$ と関数 $g:\{0,1\}^n \to \{1,-1\}$ の相関 $\mathrm{Corr}(f,g)$ は次式で定義される：

$$\mathrm{Corr}(f,g) := \left| \mathop{\mathrm{E}}_{x\in\{0,1\}^n}[f(x)g(x)] \right|$$

$$= \left| \Pr_{x\in\{0,1\}^n}[f(x)=g(x)] - \Pr_{x\in\{0,1\}^n}[f(x)\neq g(x)] \right|.$$

すなわち，全ての入力に対して，関数の出力が一致する割合と，一致しない割合との差が相関である．例として，次の場合の関数 f と関数 g の相関を考える：

- すべての $x\in\{0,1\}^n$ で $f(x)=g(x)$ となるとき，$\mathrm{Corr}(f,g)=|2^n/2^n-0|=1$.
- すべての $x\in\{0,1\}^n$ で $f(x)\neq g(x)$ となるとき，$\mathrm{Corr}(f,g)=|0-2^n/2^n|=1$.
- 全体の半分の $x\in\{0,1\}^n$ で $f(x)=g(x)$ となるとき，$\mathrm{Corr}(f,g)=\left|2^{n-1}/2^n-2^{n-1}/2^n\right|=0$.

つまり，相関が 0 から 1 までの値を取り，0 に近いほど g が f を近似できていないことを示している．

関数 f と関数のクラス C との相関 $\mathrm{Corr}(f,C)$ は，

$$\mathrm{Corr}(f,C) := \max_{g\in C}\mathrm{Corr}(f,g)$$

で定義される．f と C の相関が 0 に近ければ，f を近似する関数が C の元には存在しないことを示している．すなわち，f と C の相関の上界は，C による f の近似性の下界を示している．

計算量理論では，特別な関数と低次多項式の相関を求める研究が古くから行われてきた（表 1）．相関は，それ自身で関数の平均的な難しさを測る尺度となるが，計算量理論においてさまざまな応用がある．その 1 つとして，polynomial method を用いた計算量クラスの下界の証明が挙げられる．具体的には，

1. 低次多項式 p と計算量クラス C の相関が高い
2. 関数 f と低次多項式 p の相関が低い

を示せば，もし $f\in C$ なら 2 に矛盾するので，$f\notin C$ であることがわかる．

polynomial method は，主に段数が小さい回路クラスに対して適用される．その主な例として，Razborov による多数決関数 MAJ が AC^0（無制限ファンイン，定数段，多項式サイズの回路クラス）に含まれないことの証明 [11] と，Smolensky による剰余関数 MOD_m が $\mathrm{AC}^0(q)$（MOD_q ゲートを加えた AC^0 回路）に含まれない（m と q は互いに素）ことの証明 [14] が挙げられる．Razborov は，

1. GF(2) 上の次数 $\mathrm{poly}(\log n)$ 以下の多項式と AC^0 回路の相関が高い

2. MAJ 関数と GF(2) 上の次数 poly(log n) 以下の多項式の相関が低い

ことを示し，そこから MAJ $\notin$ AC^0 であることを導いた．ここで，1 における次数 poly(log n) は現在まで改善されていないので，polynomial method による $f \notin AC^0$ の証明では，f と次数 poly(log n) 以上の多項式の相関を求めなければいけない．

次数が poly(log n) より小さい多項式に関する相関も，回路計算量への応用がある．Alon と Beigel は，m と q が互いに素な自然数であれば，MOD_m 関数と定数次数で $\mathbb{Z}_q$ 上の多項式の相関が，定数より真に小さいことを示した．また，彼らは Hajnal 等が示した "ϵ-識別器補題" [10] をこの結果に適用すると，MAJ $\circ$ MOD_q $\circ$ AND_d 回路で MOD_m を計算する際に必要な回路サイズの下解が得られることを示唆した [2]．MAJ $\circ$ MOD_q $\circ$ AND_d 回路は，出力段に多数決ゲート，中間段に MOD_q ゲート，入力段にファンインが d 以下の AND ゲートを持つ 3 段の回路で，d が poly(log n) かつ準多項式サイズの回路であれば，AC^0 回路で計算できる全ての関数を計算することができる [1]．

MOD_m 関数と $\mathbb{Z}_q$ 上の多項式の相関が，指数関数的に小さいことを初めて示したのは Bourgain である．Bourgain は，MOD_m 関数と $\mathbb{Z}_q$ 上の多項式を指数関数の和で置き換え，それを評価することで証明した [4]．Bourgain の証明には誤りがあったが，Green, Roy, Straubing が誤りを修正した [9]．さらに，Chattopadhyay が同様のテクニックを用いて Green 等の結果を改良した [5]．

Viola と Widgerson は，Bourgain 等とは異なったテクニックで，m が奇数のとき MOD_m 関数と GF(2) 上の多項式の相関が指数関数的に小さいことを示した [15]．この証明では，Bourgain 等と同じく，MOD_m 関数を指数関数の和で置き換えているが，それを評価するために，Gowers 一様性と呼ばれる概念を導入している．Gowers 一様性は，フーリエ解析と組合せ論のアイディアを用いて定義された概念で，Szemerédi の定理の別証を与える際に Gowers によって導入された [6, 7] ものだが，多項式に対する疑似乱数生成器 [3] や PCP の線形性判定 [12, 13] など，近年，計算量理論の分野でもいくつかの応用がある．Gowers 一様性の特徴として，低次多項式との相性が非常によいことが挙げられる．具体的には，d 次多項式の $d+1$ 次 Gowers 一様性は 1 となる [8]．また，Gowers 一様性が関数の期待値で定義されていることから，互いに素な入力をとる関数 f, f' の積で定義された関数の Gowers 一様性を，各関数 f, f' の Gowers 一様性の積に分解することができる [15]．これらの性質を使うことによって，指数関数の和を直接評価するより容易に相関を評価できる．なお，Gowers 一様性は任意の加法群上で定義されるが，この証明では GF(3) 上の Gowers 一様性を用いている．

本研究では，m が 3 と互いに素な自然数のとき，MOD_m 関数と GF(3) 上の低次多項式の相関が，指数関数的に小さくなることを示した．この上界は，Chattopadhyay による結果の特殊ケース ($q = 3$) の改善となっている．この証明は，Viola と Widgerson

表 1　f と d 次多項式 p の相関

	f	d 次多項式 p	Corr(f, p)
Razborov	AC^0 の回路	GF(2) 上	$\geq 1 - 1/n^{\omega(1)}$
Razborov	MAJ	GF(2) 上	$\leq O(1/\sqrt{n})$
Alon & Beigel	MOD_m	$\mathbb{Z}_q$ 上	o(1)
Bourgain, Green et al.	MOD_m	$\mathbb{Z}_q$ 上	$\leq \exp(-\Omega(n/(q2^q)^d))$
Chattopadhyay	MOD_m	$\mathbb{Z}_q$ 上	$\leq \exp(-\Omega(n/(q2^{q-1})^d))$
Viola & Widgerson	MOD_m	GF(2) 上	$\leq \exp(-\Omega(n/4^d))$
今回の結果	MOD_m	GF(3) 上	$\leq \exp(-\Omega(n/3^d))$

による証明と同じく，Gowers 一様性を用いている．証明の方針を次に示す：

1. MOD_m 関数を，$f(x_1,\ldots,x_n)=e(x_1)\ldots e(x_n)$ のように 1 ビット関数 e で分解できる関数 f で近似する：

$$\mathrm{Corr}(\mathrm{MOD}_m,p)\approx\mathrm{Corr}(f,p).$$

2. 相関を f の Gowers 一様性 $U(f)$ で抑える：

$$\mathrm{Corr}(f,p)\le U(f).$$

3. f の Gowers 一様性を 1 ビット関数 e の一様性 $U(e)$ に分解する：

$$U(f)=U(e)^n.$$

4. e の一様性を直接計算する：

$$U(e)^n\le\exp(-\Omega(n/3^d)).$$

ここで，1 から 3 までは Viola と Widgerson の証明と同じ流れだが，4 では GF(3) 上の Gowers 一様性を計算する必要がある．そのため，GF(2) 上の Gowers 一様性より，複雑な解析が必要となる．また，この結果を前に述べた "ϵ-識別機補題" [10] に適用すると，$\mathrm{MAJ}\circ\mathrm{MOD}_3\circ\mathrm{AND}_d$ 回路で MOD_m を計算するときの下界を求めることができる．

2 諸定義

まず，本文中に現れる記法などの定義を行う．剰余関数 MOD_m は次で定義される：

$$\mathrm{MOD}_m(x_1,\ldots,x_n)=\begin{cases}1 & m\mid\sum_{i=1}^n x_i\\ -1 & m\nmid\sum_{i=1}^n x_i\end{cases}.$$

GF(3) を標数 3 の有限体とする．回路計算量理論の分野では，GF(3) 上の多項式 p を，多項式 $g:\{0,1\}^n\to\mathbb{Z}$ を用いて，

$$p(x_1,\ldots,x_n)=\begin{cases}1 & 3\mid g(x_1,\ldots,x_n)\\ -1 & 3\nmid g(x_1,\ldots,x_n)\end{cases}$$

と定義する（$x_1,\ldots,x_n\in\{0,1\}$）ことが一般的であるが，今回は次に示す Gowers 一様性との関係から，変数 $x_1,\ldots,x_n$ が GF(3) の元となるように上の定義を変更する．すなわち，GF(3) 上の多項式 p を，多項式 $g:\mathrm{GF}(3^n)\to\mathrm{GF}(3)$ を用いて，

$$p(x_1,\ldots,x_n)=\begin{cases}1 & (g(x_1,\ldots,x_n)=0)\\ -1 & (g(x_1,\ldots,x_n)\neq 0)\end{cases}$$

と定義する．多項式 p の次数は，多項式 g の次数で定義する．次数 d 以下の GF(3) 上の多項式の集合を，P_d で表すこととする．

次に，本研究で重要な役割を果たした Gowers 一様性 [6, 7] について説明する．Gowers 一様性は，任意の加法群上の関数に対して定義できるが，今回は GF(3) 上の関数に対する Gowers 一様性を用いる．

定義 1 (GF(3) 上の Gowers 一様性 [6, 7])．$d\ge 0$，$f:\mathrm{GF}(3^n)\to\mathbb{C}$，$\oplus$ を GF(3) 上の加法とする．このとき，f の GF(3) 上の d 次 Gowers 一様性 $U^d(f)$ を

$$U^d(f):=\mathop{\mathrm{E}}_{\substack{x,y_1,\ldots,y_d\\ \in\{0,1,2\}^n}}\left[\prod_{S\subseteq[d]} f\left(x\oplus\bigoplus_{j\in S}y_j\right)^{|S|}\right]$$

で定義する．ただし，$[d]$ は自然数の集合 $\{1,\ldots,d\}$ を表す．また，複素数 z と整数 i に対して，z^i は i が偶数のとき複素数 z，i が奇数のとき共役な複素数 $\bar{z}$ を表す．

Gowers 一様性は，次のような有用な性質を持っている [8, 15]．

命題 2 ([8, 15])．$f:\mathrm{GF}(3^n)\to\mathbb{C}$，$f':\mathrm{GF}(3^{n'})\to\mathbb{C}$ に対して，次の性質が成り立つ．

1. $\left|\mathop{\mathrm{E}}_{x\in\mathrm{GF}(3^n)}[f(x)]\right|=U^1(f)$.
2. 任意の自然数 k に対して，

$$U^k(f)\le\sqrt{U^{k+1}(f)}.$$

3. 次数 d 以下の GF(3) 上の多項式 p に対して，

$$U^{d+1}(f\cdot p)=U^{d+1}(f).$$

4. $(f\cdot f')(x,y):=f(x)\cdot f'(y)$ とすると，

$$U^k(f\cdot f')=U^k(f)\cdot U^k(f').$$

3 MOD_m と GF(3) 上の多項式の相関

本章では，本研究の結果である剰余関数 MOD_m と GF(3) 上の低次多項式の相関を評価する．次に掲げる定理 3 で，この相関が低いことを示す．

定理 3.

$$\mathrm{Corr}(\mathrm{MOD}_m, P_d) \le \exp\left(-\alpha \cdot \frac{n}{3^d}\right).$$

ただし，m は 3 と互いに素な自然数で，$\alpha(>0)$ は m に依存する定数．

証明. $e_m(x) := \exp\left(\frac{2\pi i}{m} \cdot x\right)$ と定義する．

$$\sum_{a=1}^{m-1} e_m\left(a \cdot \sum_{i=1}^{n} x_i\right) = \begin{cases} m-1 & \left(m \mid \sum_{i=1}^{n} x_i\right) \\ -1 & \left(m \not\mid \sum_{i=1}^{n} x_i\right) \end{cases}$$

となるので，$f(x) := e_m\left(\sum_{i=1}^{n} x_i\right)$ とおくと，

$$\mathrm{MOD}_m(x_1, \ldots, x_n) = -\mathrm{sgn}\left(\sum_{a=1}^{m-1} f(x)^a\right)$$

を満たす．つまり，$\mathrm{MOD}_m(x)$ を $\sum_a f(x)^a$ で置き換えることができる．このことから，

$$\begin{aligned} &\mathrm{Corr}(\mathrm{MOD}_m, p) \\ &\le \mathop{\mathrm{E}}_{x \in \mathrm{GF}(3^n)}\left[\sum_{a=1}^{m-1} f(x)^a p(x)\right] \\ &\le (m-1) \max_{1 \le a < m} \mathop{\mathrm{E}}_{x \in \mathrm{GF}(3^n)}[f(x)^a p(x)] \end{aligned}$$

となる．ここで，$k := d+1$ とおくと

$$\begin{aligned} \mathop{\mathrm{E}}_{x \in \mathrm{GF}(3^n)}[f(x)^a p(x)] &= U^1(f^a \cdot p) \\ &\le \left\{U^{d+1}(f^a \cdot p)\right\}^{1/2^{d+1}} \\ &= \left\{U^k(f^a \cdot p)\right\}^{1/2^k} \\ &= \left\{U^k(f^a)\right\}^{1/2^k} \\ &= \left\{U^k(e_m^a)\right\}^{n/2^k} \end{aligned}$$

となり，1 ビット関数 e_m^a の Gowers 一様性

$$\begin{aligned} &U^k(e_m^a) \\ &= \left| \mathop{\mathrm{E}}_{\substack{x, y_1, \ldots, y_k \\ \in \{0,1,2\}}} \left[\prod_{S \subseteq [k]} e_m\left((-1)^{|S|} \cdot a \left(x \oplus \bigoplus_{j \in S} y_j\right)\right)\right]\right| \\ &= \left| \mathop{\mathrm{E}}_{\substack{x, y_1, \ldots, y_k \\ \in \{0,1,2\}}} \left[e_m\left(\sum_{S \subseteq [k]} (-1)^{|S|} \cdot a \left(x \oplus \bigoplus_{j \in S} y_j\right)\right)\right]\right| \end{aligned}$$

を評価すればよいことがわかる．ここで，$y_1, \ldots, y_k$ を固定すると，次の 2 つの補題が成り立つ．これら 2 つの補題が，本研究の中心となる補題である．

補題 4. $y_i = 0$ となる i $(1 \le i \le k)$ が存在すれば，任意の $x \in \{0,1,2\}$ に対して，

$$e_m\left(\sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j\right)\right) = 1.$$

補題 5. 全ての i $(1 \le i \le k)$ に対し，$y_i \neq 0$ かつ k が偶数なら，

$$\sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j\right) = \begin{cases} 0 \\ 3^{\frac{k}{2}} \\ -3^{\frac{k}{2}} \end{cases}.$$

ただし，各々の値は x を $\{0,1,2\}$ から一様に選ぶと，確率 $\frac{1}{3}$ で現れる．

k が偶数のとき，これらの補題を用いて，

$$\begin{aligned} U^k(e_m^a) &= \frac{2^k}{3^{k+1}} \cdot e_m(0) + \frac{2^k}{3^{k+1}} \cdot e_m(3^{\frac{k}{2}} \cdot a) \\ &\quad + \frac{2^k}{3^{k+1}} \cdot e_m(-3^{\frac{k}{2}} \cdot a) + \left(1 - \frac{2^k}{3^k}\right) \cdot e_m(0) \\ &= 1 - \frac{3 \cdot 2^k - 2^k}{3^{k+1}} + \frac{2^{k+1}}{3^{k+1}} \cos\left(\frac{2\pi}{m} \cdot 3^{\frac{k}{2}} \cdot a\right) \\ &= 1 - \frac{2^{k+1}(1-\delta)}{3^{k+1}} \end{aligned}$$

(ただし，$\delta := \cos\left(2\pi \cdot a \cdot 3^{k/2}/m\right)$)．$m$ は 3 と互いに素で，かつ $a \in \{1, \ldots, m-1\}$ であるから $\delta < 1$．ゆえに，

$$\begin{aligned} \left\{U^k(e_m^a)\right\}^{n/2^k} &= \left(1 - \frac{2(1-\delta)}{3^{k+1}} \cdot \frac{1}{1/2^k}\right)^{n/2^k} \\ &\le \exp\left(-\frac{2(1-\delta)}{3} \cdot \frac{n}{3^k}\right) \\ &= \exp\left(-\frac{2(1-\delta)}{9} \cdot \frac{n}{3^d}\right). \end{aligned}$$

ここで，係数 $(m-1)$ と指数 $2(1-\delta)/9$ を指数 α で置き換えれば定理を得る．$\delta < 1$ より，$\alpha > 0$．k が奇数のときは，$k+1$ を k に置き換えると，同様の結果を得る． ■

次に，定理の証明中に用いた，本研究の中核を成す 2 つの補題を証明する．

補題 4 (再掲)．$y_i = 0$ となる i $(1 \le i \le k)$ が存在すれば，任意の $x \in \{0,1,2\}$ に対して，

$$e_m\left(\sum_{S\subseteq[k]}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\right) = 1.$$

証明.

$$\begin{aligned}
&\sum_{S\subseteq[k]}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\
&= \sum_{S\subseteq[k]\setminus\{i\}}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\
&\quad - \sum_{S\subseteq[k]\setminus\{i\}}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j \oplus y_i\right)\\
&= \sum_{S\subseteq[k]\setminus\{i\}}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\
&\quad - \sum_{S\subseteq[k]\setminus\{i\}}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\
&= 0
\end{aligned}$$

となるので，

$$e_m\left(\sum_{S\subseteq[k]}\left(x \oplus \bigoplus_{j\in S} y_j\right)\right) = e_m(0) = 1.$$

■

補題 5 (再掲)．全ての i $(1 \le i \le k)$ に対し，$y_i \neq 0$ かつ k が偶数なら，

$$\sum_{S\subseteq[k]}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right) = \begin{cases} 0 \\ 3^{\frac{k}{2}} \\ -3^{\frac{k}{2}} \end{cases}.$$

ただし，各々の値は x を $\{0,1,2\}$ から一様に選ぶと，確率 $\frac{1}{3}$ で現れる．

証明．$k \ge 2$ のときを考える．まず，

$$\begin{aligned}
&\sum_{S\subseteq[k]}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\
&:= \alpha_0 x + \alpha_1(x\oplus 1) + \alpha_2(x \oplus 2)
\end{aligned}$$

$(\alpha_0,\alpha_1,\alpha_2 \in \mathbb{Z}_{\ge 0},\ \alpha_0+\alpha_1+\alpha_2 = 0)$ とおくと，次の主張が成り立つ．

主張 1．$k \ge 2$ のとき，k が偶数なら

$$\{\alpha_0,\alpha_1,\alpha_2\} = \begin{cases} \{\beta_k,\beta_k,-2\beta_k\} \\ \{-\beta_k,-\beta_k,2\beta_k\} \end{cases}, \qquad (1)$$

k が奇数なら

$$\{\alpha_0,\alpha_1,\alpha_2\} = \{0,\beta_k,-\beta_k\} \qquad (2)$$

となる β_k が存在．ただし，β_k は k によって決まる自然数で，$\{\cdot\}$ は multiset.

(主張 1 の証明)．k に関する帰納法で示す．$k = 2$ のとき，

$$\begin{aligned}
&\sum_{S\subseteq[2]}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\
&= x - (x\oplus y_1) - (x\oplus y_2) + (x \oplus y_1 \oplus y_2)\\
&= \begin{cases} x - 2(x\oplus 1) + (x\oplus 2) & \text{if } (y_1,y_2) = (1,1) \\ 2x - (x\oplus 1) - (x\oplus 2) & \text{if } (y_1,y_2) = (1,2) \text{ or } (2,1) \\ x + (x\oplus 1) - 2(x\oplus 2) & \text{if } (y_1,y_2) = (2,2) \end{cases}
\end{aligned}$$

となるので，$\{\alpha_0,\alpha_1,\alpha_2\} = \{1,1,-2\}$ または $\{-1,-1,2\}$ となり，$\beta_2 := 1$ とおけば (1) は成立する．

次に，$k-1$ まで (1)，(2) が成立すると仮定する．

$$\begin{aligned}
&\sum_{S\subseteq[k-1]}(-1)^{|S|}\left(x \oplus \bigoplus_{j\in S} y_j\right)\\
&:= \alpha_0 x + \alpha_1(x\oplus 1) + \alpha_2(x \oplus 2)
\end{aligned}$$

とおくと，

$$\sum_{S\subseteq[k]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\right)$$
$$=\sum_{S\subseteq[k-1]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\right)$$
$$-\sum_{S\subseteq[k-1]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\oplus y_k\right)$$
$$=\alpha_0x+\alpha_1(x\oplus1)+\alpha_2(x\oplus2)$$
$$-\alpha_0(x\oplus y_k)-\alpha_1(x\oplus1\oplus y_k)-\alpha_2(x\oplus2\oplus y_k).$$

これは，$y_k=1$ のとき

$$(\alpha_0-\alpha_2)x+(\alpha_1-\alpha_0)(x\oplus1)+(\alpha_2-\alpha_1)(x\oplus2),$$

$y_k=2$ のとき

$$(\alpha_0-\alpha_1)x+(\alpha_1-\alpha_2)(x\oplus1)+(\alpha_2-\alpha_0)(x\oplus2)$$

となる．つまり，係数集合 $\{\alpha_0-\alpha_2,\alpha_1-\alpha_0,\alpha_2-\alpha_1\},\{\alpha_2-\alpha_0,\alpha_0-\alpha_1,\alpha_1-\alpha_2\}$ に注目すればよい．

k が偶数のとき，$k-1$ は奇数なので，$\{\alpha_0,\alpha_1,\alpha_2\}=\{0,\beta_{k-1},-\beta_{k-1}\}$．ここで，$\alpha_0=0$ とすると，

$$\alpha_0-\alpha_2=-(\pm\beta_{k-1})=\mp\beta_{k-1}$$
$$\alpha_1-\alpha_0=\mp\beta_{k-1}=\mp\beta_{k-1}$$
$$\alpha_2-\alpha_1=\pm\beta_{k-1}-(\mp\beta_{k-1})=\pm2\beta_{k-1},$$

および

$$\alpha_2-\alpha_0=\pm\beta_{k-1}=\pm\beta_{k-1}$$
$$\alpha_0-\alpha_1=-(\mp\beta_{k-1})=\pm\beta_{k-1}$$
$$\alpha_1-\alpha_2=\mp\beta_{k-1}-(\pm\beta_{k-1})=\mp2\beta_{k-1}.$$

同様に，$\alpha_1=0,\alpha_2=0$ のときも考えると，

$$\{\alpha_0-\alpha_2,\alpha_1-\alpha_0,\alpha_2-\alpha_1\}$$
$$=\{\alpha_2-\alpha_0,\alpha_0-\alpha_1,\alpha_1-\alpha_2\}$$
$$=\{\pm\beta_{k-1},\pm\beta_{k-1},\mp2\beta_{k-1}\}$$

となるので，$\beta_k:=\beta_{k-1}$ とおけば，(1) が成り立つ．

k が奇数のとき，$k-1$ は偶数なので，$\{\alpha_0,\alpha_1,\alpha_2\}=\{\pm\beta_{k-1},\pm\beta_{k-1},\mp2\beta_{k-1}\}$．ここで，$\alpha_0=\mp2\beta_{k-1}$ とすると，

$$\alpha_0-\alpha_2=\mp2\beta_{k-1}-(\pm\beta_{k-1})=\mp3\beta_{k-1}$$
$$\alpha_1-\alpha_0=\pm\beta_{k-1}-(\mp2\beta_{k-1})=\pm3\beta_{k-1}$$
$$\alpha_2-\alpha_1=\pm\beta_{k-1}-(\pm\beta_{k-1})=0,$$

および

$$\alpha_2-\alpha_0=\pm\beta_{k-1}-(\mp2\beta_{k-1})=\pm3\beta_{k-1}$$
$$\alpha_0-\alpha_1=\mp2\beta_{k-1}-(\pm\beta_{k-1})=\mp3\beta_{k-1}$$
$$\alpha_1-\alpha_2=\pm\beta_{k-1}-(\pm\beta_{k-1})=0.$$

同様に，$\alpha_1=0,\alpha_2=0$ のときも考えると，

$$\{\alpha_0-\alpha_2,\alpha_1-\alpha_0,\alpha_2-\alpha_1\}$$
$$=\{\alpha_2-\alpha_0,\alpha_0-\alpha_1,\alpha_1-\alpha_2\}$$
$$=\{0,\pm3\beta_{k-1},\mp3\beta_{k-1}\}$$

となるので，$\beta_k:=3\beta_{k-1}$ とおけば，(2) が成り立つ． ■

ここで，

$$\beta_k=\begin{cases}1 & (k=2)\\ \beta_{k-1} & (k\text{: 偶数})\\ 3\beta_{k-1} & (k\text{: 奇数})\end{cases}$$

より，

$$\beta_k=3^{\lceil\frac{k-2}{2}\rceil}. \tag{3}$$

$x,x\oplus1,x\oplus2\in\{0,1,2\}$ より，k が偶数のとき，

$$\sum_{S\subseteq[k]}(-1)^{|S|}\left(x\oplus\bigoplus_{j\in S}y_j\right)=\begin{cases}\pm3\beta_k\\ \mp3\beta_k\\ 0\end{cases},$$

となるので，これに (3) を代入すると補題が導ける． ■

4 回路計算量への応用

本章では，次の形で定義される相関を用いる．

$$\mathrm{corr}(f,g)$$
$$:=\left|\Pr_{\substack{x\in\{0,1\}^n\\ f(x)=-1}}[g(x)=-1]-\Pr_{\substack{x\in\{0,1\}^n\\ f(x)=1}}[g(x)=-1]\right|.$$

観察．この相関を用いても，定理 3 と同様の上界を得ることができる．これは，

$$\mathrm{corr}(\mathrm{MOD}_m,p)\le\mathrm{O}(m)\left|\mathop{\mathrm{E}}_{x\in\{0,1\}^n}[f(x)^ap(x)]\right|+2^{-\epsilon n}$$

($\epsilon>0$) が Bourgain によって示されている [4] ので，定理 3 で示した上界と定数倍しか変わらないためである．

この形で定義された相関は，閾値回路の下界を含意している．それを示したのが，次に掲げる "ϵ-識別器" 補題である．

補題 6 (ϵ-識別器 [10]). C を重み無し閾値ゲートに，部分回路 $c_1, \ldots, c_s$ の出力を入力することで構成される回路とする．すなわち，

$$C(x) = 1 \iff \sum_{i=1}^{s} c_i(x) \geq t$$

(ただし $t \in \mathbb{N}$)．このとき，

$$s \cdot \max_{1 \leq i \leq s} \mathrm{corr}(C, c_i) \geq 1$$

となる．

定理 3 で得られた相関の上界を補題 6 の対偶に適用すると，系 7 に掲る $\mathrm{MAJ} \circ \mathrm{MOD}_3 \circ \mathrm{AND}_d$ 回路で MOD_m を計算する際の下解が得られる．$\mathrm{MAJ} \circ \mathrm{MOD}_3 \circ \mathrm{AND}_d$ 回路とは，出力段に多数決ゲート，中間段に MOD_3 ゲート，入力段にファンインが d 以下の AND ゲートを配置した 3 段の回路である．なお，Allender によって，$d = \mathrm{poly}(\log n)$ のとき，AC^0 回路で計算できる任意の関数が，$n^{\mathrm{O}(\log^k n)}$ サイズの $\mathrm{MAJ} \circ \mathrm{MOD}_3 \circ \mathrm{AND}_d$ 回路で計算できることが示されている [1].

系 7. $\mathrm{MAJ} \circ \mathrm{MOD}_m \circ \mathrm{AND}_d$ 回路が MOD_3 を計算するとき，MAJ ゲートへのファンインは $\exp(\alpha \cdot \frac{n}{3^d})$ 必要.

5 結論と未解決問題

本研究では，MOD_m 関数と GF(3) 上の多項式の相関が高々 $\exp(-\alpha n/3^d)$ であることを，Gowers 一様性を用いて示した．この結果は，既存の上界を改善している．

Gowers 一様性を用いた，MOD_m 関数と GF(5) 上の多項式の相関の評価は未解決である．GF(5) 上における e_m 関数の Gowers 一様性は，$x, y_1, \ldots, y_k \in \{0,1,2,3,4\}$ に関する

$$e_m\left(\sum_{S \subseteq [k]} (-1)^{|S|} \left(x \oplus \bigoplus_{j \in S} y_j\right)\right)$$

の期待値で与えられるが，この場合は補題 5 のように，$y_1, \ldots, y_k$ を固定してもこの値は一意には定まらない．そのため，この期待値を求めるのは困難である．

また，多項式の次数 d が $\mathrm{poly}(\log n)$ であるとき，本研究の評価法では自明な上界しか求められない．この場合の上界がどのような値になるかも未解決である．

参考文献

[1] E. Allender, A Note on the Power of Threshold circuits, 30th Ann. Symp. Foundations Comput. Sci., pages 514-519, 1989.

[2] N. Alon, R. Beigel, Lower Bounds for Approximation by Low Degree Polynomials over $\mathbb{Z}_m$, Annual IEEE Conference on Computational Complexity vol. 16, 2001.

[3] A. Bogdanov and E. Viola, Pseudorandom Bits for Polynomial, 48th Ann. Symp. Foundations Comput. Sci., pages 41-51, 2007.

[4] J. Bourgain, Estimation of Certain Exponential Sums Arising in Complexity Theory, C. R. Math. Acad. Sci. Paris, 340(9), pages 627-631, 2005.

[5] A. Chattopadhyay, An Improved Bound on Correlation between Polynomials over $\mathbb{Z}_m$ and MOD_q, Electronic Colloquium on Computational Complexity, Technical Report TR06-107, 2006.

[6] W. T. Gowers, A New Proof of Szemerédi's Theorem for Arithmetic Progressions of Length Four, Geom. Funct. Anal., 8(3), pages 529-551, 1998.

[7] W. T. Gowers, A New Proof of Szemerédi's Theorem, Geom. Funct. Anal., 11(3), pages 465-588, 2001.

[8] B. Green and T. Tao, An Inverse Theorem for the Gowers $U^3(G)$ Norm, 2005. arXiv.org:math/0503014.

[9] F. Green, A. Roy, and H. Straubing, Bounds on an Exponential Sum Arising in Boolean

Circuit Complexity, C. R. Math. Acad. Sci. Paris, 341(5), pages 279-282, 2005.

[10] A. Hajnal, W. Maass, P. Pudlak, M. Szegedy, and G. Turan, Threshold Circuits of Bounded Depth, J. Comput. System Sci., 46(2), pages 129-154, 1993.

[11] A. A. Razborov, Lower Bounds on the Dimension of Schemes of Bounded Depth ina Complete Basis Containing the Logical Function, Mat. Zametki, 41(4), pages 598-607, 623, 1987.

[12] A. Samorodnitsky, Low Degree Tests at Large Distances, 2006, Manuscript.

[13] A. Samorodnitsky and L. Trevisan, Gowers Uniformity, Influence of Variables, and PCPs, In Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing 2006, pages 11-20, 2006.

[14] R. Smolensky, Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity, In Proc. 19th Ann. ACM Symp. Theor. Comput., pages 77-82, 1987.

[15] E. Viola and A. Wigderson, Norms, XOR Lemmas, and Lower Bounds for GF(2) Polynomials and Multiparty Protocols, CCC '07: Proceedings of the Twenty-Second Annual IEEE Conference on Computational Complexity, pages 141–154, 2007.